DEPARTMENT OF THE AIR FORCE

AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GCS/ENG/88D-23

A CLASS C2 SECURITY EVALUATION PROCEDURE FOR LOCAL AREA NETWORKS

THESIS

Rick E. Whitson
Captain, USAF

AFIT/GCS/ENG/88D-23

Approved for public release; distribution unlimited

AFIT/GCS/ENG/88D-23

A CLASS C2 SECURITY EVALUATION PROCEDURE FOR LOCAL AREA NETWORKS

THESIS

Presented to the Faculty of the School of Engineering
of the Air Force Institute of Technology
Air University
In Partial Fulfillment of the
Requirements for the Degree of
Master of Science in Computer Systems

Rick E. Whitson, B.S.
Captain, USAF

December 1988

Preface

This thesis was undertaken to provide a consistent, straight forward methodology for Local Area Network (LAN) security evaluations. An evaluation is distinctly different from a risk or vulnerability assessment. Before a LAN can be authorized to process sensitive or classified information, it must go through an accreditation process which includes the risk and vulnerability assessment. Information on system accreditation can be found in Air Force Regulation 205-16.

The National Computer Security Center's (NCSC's) security criteria are used to setup a checklist for class C2 evaluations. A complete description of class C2 criteria can be found in chapter II and references 3 and 4.

I would like to thank Maj Bill Thomas at HQ USAF/SCTT, Capt Jerry Cogar at AFCSC and Dr David Vaughan at AFIT for their help and support in this thesis effort. In addition, I would like to express my deep appreciation to my wife for her support and understanding during these eighteen months.

Table of Contents

List of Figures

Glossary

AFCSC	Air Force Cryptologic Support Center
AFR	Air Force Regulation
AI	Combination of Audit and Identification-Authentication components
DA	Combination of Discretionary Access Control and Audit components
DAC	Discretionary Access Control
DI	Combination of Discretionary Access Control and Identification/Authentication components
DoD	Department of Defense
ESC	Electronic Security Command
IAD	Combination of Identification/Authentication, Audit and Discretionary Access Control components
LAN	Local area network
NCSC	National Computer Security Center
NSAD	Network security architecture and design
NTCB	Network trusted computing base
Object	An entity that contains or receives information
Sponsor	Individual or entity responsible for presenting the LAN for evaluation
Subject	An active entity, usually in the form of a user or processes started by users, also includes processes that move information or change the state of an object
TCB	Trusted computing base
TFM	Trusted facility manual

Abstract

The National Computer Security Center's (NCSC) Computer Security Requirements, CSC-STD-003-85 (Yellow Book) specifies "Class C2" as the required protection level for computer systems running at a "system high" level of Top Secret. Methodology exists to determine if a computer system provides class C2 protection, however, there are no general procedures available to determine if a Local Area Network (LAN) provides class C2 protection.

This thesis effort reviewed the criteria necessary for a C2 rating and developed a checklist based on the three types of security features required (discretionary access control, identification/authentication and audit capabilities) in a C2 system. HQ USAF/SCTT and the Air Force Cryptologic Support Center (AFCSC) reviewed the proposed checklist to identify deficiencies and inconsistencies. Their comments were addressed and the checklist modified as required. The checklist was then applied to a LAN used in the US Air Force to verify the capabilities of the checklist and determine if the LAN provided class C2 protection. Problems in applying the checklist were identified and changes were incorporated into the checklist. The checklist can now be used to determine if a LAN provides class C2 security.

A CLASS C2 SECURITY EVALUATION PROCEDURE FOR LOCAL AREA NETWORKS

I. Introduction

Background

There is a growing requirement in the Air Force to interconnect personal computers (PCs). Interconnection streamlines office communications, simplifies paperwork, and allows more efficient use of personnel. Interconnection provides the data communication features of a modem and in addition can provide sharing of data files, application programs, expensive computer peripherals as well as mail and calendar services.

Interconnection takes place on local area networks (LANs). A LAN includes a physical medium (coaxial cable, twisted pair, or optical fiber) and communications software to connect computers and computer peripherals into a logical entity. The communications software runs on devices dedicated for LAN services as well as on the interconnected PCs.

LANs are being installed at an ever increasing rate to capitalize on the benefits PC interconnection provides. But the additional features provided by LANs (sharing data and

applications on a PC with every other PC on the LAN) bring into focus security issues that must be addressed.

Sensitive and classified information must be protected from unauthorized access, yet the protection methodology must be flexible enough to allow access by authorized users on a case by case basis. Mainframe computers control access to their resources with software and hardware and procedures exist to determine if mainframes provide the security controls necessary for the protection of their data.

PCs generally do not provide access control and there are no general procedures available for determining whether a LAN provides the security controls necessary to protect the data being processed (1:3.6). Therefore, when PCs are interconnected through a LAN, there is no well defined procedure for determining the security protection provided. This problem was recently reemphasized in conversations with the Air Force Cryptologic Support Center's Computer Security Branch (AFCSC/SRVC) and HQ USAF/SCTT. They stated that determining a LANs security capabilities was a difficult problem with no well defined solution.

At this time, agencies, responsible for certifying LANs to process sensitive or classified information, develop new evaluation procedures for each LAN requiring certification. A standardized procedure would save time, avoid duplication of effort, and provide consistent evaluation criteria for LAN evaluations.

The National Computer Security Center (NCSC) provides security guidance relating to the hardware and software capabilities required for protection of the information available on a computer system or network (2:1-38). The security-relevant portions of a computer system are referred to as the Trusted Computing Base (TCB) (3:5). The security-relevant portions of a LAN are referred to as the Network Trusted Computing Base (NTCB), which is partitioned among the network components to ensure the overall network security policy is enforced by the network as a whole (4:xiv).

The NCSC has established four protection divisions for TCBs and NTCBs (divisions A, B, C, and D). Division A provides the most stringent protection criteria and includes only one class, A1. Division B contains three classes (B1, B2, and B3) and division C contains two classes (C1 and C2). Increasing class numbers in a division relate to more stringent security requirements (C2 requires more security controls than C1). Division D is reserved for systems or networks which do not meet division A, B, or C's requirements and is considered to provide minimal protection. The required criteria in each division and class are explained in Chapter II.

The sponsor of this thesis effort, Headquarters Electronic Security Command (HQ ESC/SC-OA), employs LANs in a "system high" Top Secret (TS) environment. A "system

high" environment is one in which the system and all the information on the system are protected commensurate with the highest level of information processed. A "system high" environment also requires that all users of the system hold a security clearance equal to or greater than that of the system.

In a "system high" mode, if a LAN processes any TS data, the LAN and all the data on it are regarded as TS. A network in a "system high" TS environment should operate at NCSC's evaluation class C2 (2:13).

Problem

ESC needs to know if their LANs' security capabilities meet the specifications for security at class C2. Therefore, this thesis effort develops a general procedure for measuring a LAN's security relevant characteristics against NCSC's class C2 security criteria. Once developed, the procedure will be used to evaluate ESC's LAN.

Assumptions

The major assumption in undertaking this project was that it was possible to develop a usable, general methodology comparing a LAN's security capabilities against class C2 criteria.

Procedures have been developed for determining the protection levels provided by computer systems. A LAN can be thought of as an extended computer system. It is more

complex and generally larger, but it can be considered a computer system none the less. Therefore, it was felt a general procedure to evaluate LANs at class C2 could be developed.

Scope

HQ ESC/SC-OA needed to know whether or not its LANs met class C2 criteria. Therefore, this effort was restricted to the development of a procedure for analyzing security issues at class C2. In the future, it will be necessary to evaluate LANs at the higher security protection divisions (B and A). But as the security requirements become more stringent, the procedures necessary for LAN evaluations become more ponderous, complicated, and complex. The increased complexity required in evaluations of the higher divisions make general procedures difficult to develop and verify that they function as required.

Methodology/Standards

The first step was to define the criteria a LAN must meet to provide class C2 protection. Once NCSC's security criteria were understood and defined, a general procedure could be developed. The procedure was adapted as a checklist which provides a step by step approach for LAN evaluations. The checklist can be found in the appendix.

Difficulty in developing a checklist results from the subjective nature of NCSC's requirements for a class C2

system. Once developed, the checklist was evaluated by the Air Force Cryptologic Support Center (AFCSC/SRER), AFCSC/SRVC, and HQ USAF/SCTT for deficiencies or inconsistencies and to verify that the interpretation of the NCSC criteria in the checklist met the AF's interpretation of the criteria. The responses received from HQ USAF/SCTT and AFCSC were evaluated and changes were made to the checklist alleviating the identified problem areas.

Difficulty in applying the checklist occurs because the NCSC requirements do not specify solutions to meet specific criteria. They specify only the features required for a C2 rating and the required features can be provided by many different designs, interfaces and protocols. The checklist identifies the criteria that a LAN must satisfy to be considered C2, but the checklist does not specify how the required features must be implemented, nor how the implemented features must interact to meet the security requirements. Before an evaluation can begin, the evaluator(s) must understand the security capabilities and design of the LAN.

After the checklist was applied to ESC's LAN, the checklist was modified to eliminate as many problem areas as possible without changing the features or capabilities of the checklist.

Summary

A checklist was developed to evaluate a LAN's security capabilities at class C2. The NCSC criteria for a C2 rating are explained in chapter II and the checklist design and development based on the criteria was accomplished in chapter III.

After the checklist was developed, the security capabilities of a LAN provided by ESC's LAN were evaluated using the checklist. The evaluation development and results are in chapter IV; areas where class C2 were not met were identified explicitly with possible solutions to correct the problems identified where possible. In addition, any problems in applying the checklist (procedure) were identified and the checklist was modified to eliminate the problem areas.

Chapter V presents the conclusions and recommendations reached in the previous four chapters. The checklist itself can be found in the appendix. The checklist was placed in the appendix so it could be easily removed from the thesis document and used as a guide in future LAN evaluations.

II. NCSC's Protection Criteria for a C2 Network

Overview of NCSC's Security Guidance

The National Computer Security Center (NCSC) provides the standards and guidance, within DoD, relating to hardware and software security capabilities required for the protection of sensitive and classified information on computer systems or computer networks. NCSC's overall goal is to:

1. Provide a standard to industry as to the security features required for systems handling sensitive or classified information.

2. Provide evaluation criteria to measure industries' compliance to the standard and the degree of trust that can be placed in the system.

3. Set a basis for specifying security requirements in acquisition/procurement specifications. (3:2)

Their publications include:

1. Security protection levels required in relation to different sensitivity levels (sensitive, confidential, secret, top secret) processed on a system.

2. The features (criteria) required in the system to meet the specified protection level.

3. Additional guidance on and explanations of the required features.

A list of NCSC's publications can be obtained by contacting:

Department of Defense/Attn: S932
National Security Agency
9800 Savage Road
Fort Mead, Md.
20755-6000

Overview of NCSC's Security Criteria

The NCSC established four protection divisions, A, B, C and D with division A providing the most stringent protection criteria and division D providing only minimal protection.

Division A provides the most comprehensive security protection (Verified Protection). It is difficult to implement and difficult to evaluate. The definition of division A follows.

> Division A requires the use of formal security methods to assure that the mandatory and discretionary security controls, employed in the network system, can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the NTCB meets the security requirements in all aspects of design, development, and implementation. (4:125)

Division B (Mandatory Protection) requires more stringent controls and testing than Division C but is easier to develop and evaluate than Division A. Division B is based on the integrity of required sensitivity labels. It uses sensitivity labels to enforce a set of "mandatory" access control rules (2:23). The sensitivity labels must be carried with all information in the network. The sponsor must provide a security policy model on which the Networked

Trusted Computing Base (NTCB) is based and furnish the specification for the NTCB. The sponsor is the individual or entity responsible for presenting a component or LAN for evaluation and could be a manufacturer developer or program manager (4:x). The NTCB is the hardware and software providing the security protection for the system.

Division B contains 3 classes (B1, B2, and B3). Class B1 requires the features specified at the division level. Class B2 and B3 require more stringent controls and move beyond the basic requirements toward the requirements of Division A.

Division C must provide discretionary (need-to-know) protection, identification/authentication capabilities, and accountability of subjects (users and processes started by them) and the actions they initiate, via audit capabilities. Audit capabilities are used to track a subject's use or modification of an object, providing a means of holding users (subjects) accountable for their actions. Class C1 requires the features of Division C but does not require an audit trail. Class C2 enforces a more stringent discretionary access control (DAC) than C1 by requiring auditing of security-relevant events and resource encapsulation.

Division D is reserved for those systems or LANs that do not meet one of the preceding divisions and is considered to provide only minimal protection.

Class C2

Class C2 is the level of protection required for ESC's LAN and the checklist was developed for LAN evaluations at this level. Therefore, class C2 will be reviewed in detail. A LAN at class C2 must:

1. Separate users and data.

2. Allow users to protect project or private information.

3. Make users accountable for their actions via audit trails.

4. Encapsulate resources. (2:23-24)

To support the above requirements, the NTCB must satisfy four main areas:

1. There must be a "Security Policy" giving a description of the overall network security as it relates to users, data, and applications.

2. Users must be "Accountable" for their actions. Accountability requires the security software to provide audit information on actions invoked by a user. Therefore, users must identify and authenticate their identities before using the system.

3. There must be "Assurance" that the NTCB will protect itself from external interference or tampering and isolate all resources it protects.

4. There must be separate "Documentation" manuals provided for users, system administrator(s), hardware/software setup and security testing. (4:16-29)

Security Policy. The sponsor of the network must describe the overall network security policy enforced by the NTCB, including:

1. Procedures for protecting the information being processed based on the authorizations of users or groups of users.

2. An access control policy describing network requirements to prevent or detect the "reading or destroying" of sensitive information by unauthorized users or errors in the system.

Unauthorized users are those not authorized to use the network, as well as legitimate users not authorized access to a specific piece of protected data (4:16).

The NTCB is required to control the reading and writing of shared information to be considered a trusted network. Control of reading is used to protect sensitive information (data secrecy) while control of writing is used to protect against the destruction or modification of information (data integrity), giving a network the ability to protect the secrecy and integrity of information entrusted to it. This trust is required while information is being processed or transmitted on the network (4:17).

The NTCB will define and control access between named users and named objects. The access control mechanism, by explicit action or by default, must protect objects from unauthorized access. Access permission to an object will be granted only by authorized users (security managers or the owner of private data). If access is granted to a group of individuals, the audit trail must reflect the users

represented by the group identifier (4:18). If an object, such as a hard disk, is to be reused (placed in service for access by subjects) all authorizations to the information contained on it must be revoked prior to reuse.

Accountability. Users must identify and authenticate their identity to the NTCB. The identity and authentication can be implemented using unique names (user-IDs) for their identity and a protected mechanism (password) for authentication purposes. The identification and authentication process may be required to utilize each component on the network or, if a device is acting as the identification and authentication server for the network, be required only when service is initiated (4:20-21).

The NTCB is required to enforce individual accountability by providing the ability to uniquely identify an individual user. This identity will provide the NTCB the capability to create audit information on actions taken by a user. When audit information is created, the NTCB will maintain and protect it from modification. Only those system administrators with specific authentication will be able to read or modify audit information. The following types of events will be auditable: use of identification and authentication mechanisms, introduction of objects to a user's address space (creation of objects), deletion of objects, actions taken by computer operators and system administrators/security officers, and any other security

relevant events (4:22). The audit trail will identify the date and time of the event, user ID, type of event and the success or failure of the event. For identification/ authentication events, the location of request will be included. For additions and deletions of objects, the audit trail will include the object name.

Assurance. The NTCB must maintain a domain for its own execution to protect it from external interference or tampering, whether the NTCB is located at a central location or partitioned across the network. The NTCB will also isolate the resources it protects, making them subject to all access control and auditing requirements (4:23).

Any communication between NTCB partitions must also be protected. Cryptographic checksums and physical security are two possible methods of protecting communications between partitions. If the NTCB is partitioned, the partitions must have the ability to communicate and periodically validate each other's responses. If an invalid response is received, NTCB partitions will report any failures detected to the network system administrators (4:24). The partitions must also isolate all resources within their respective partitions requiring protection.

The security mechanisms must be tested to exercise all the interfaces and protocols of a component and verify the NTCB functions as claimed in the system documentation (4:25). The tests should include integrated testing

involving all components containing NTCB partitions. They should include tests to search for obvious flaws which would allow violation of resources or unauthorized access to the audit or authentication data.

Documentation. User documentation will be provided describing the visible protection provided by the NTCB to the user. The user interfaces provided by components, the interaction among components and instructions on how users interact with the security components will also be included in the user documentation.

Documentation must also be provided for the NTCB system administrator(s). This manual (Trusted Facility Manual, TFM) will contain specifications and procedures to assist the system administrator(s) in maintaining the network and will include:

1. Supported hardware configurations.
2. Implications of attaching new components.
3. Implications of removing components or losing them due to device failure.
4. Network configuration aspects that can impact the security of the system (what features must be protected).
5. Information on loading or modifying NTCB software.
6. Procedures for examining and maintaining audit files. (4:26)

The Trusted Facility Manual must also include the physical and administrative environmental controls required by the network (4:26); assumptions about the security of a given

network should be clearly stated (TEMPEST considerations, required physical security). A description of external security controls can be found in Air Force Regulation 205-16.

A Network Security Architecture and Design (NSAD) document must also be provided. The Network Security Architecture explains the security-relevant policies, objectives, and protocols (4:28). It provides information on the security features in the network and which devices or components of the LAN provide which security features. It specifies the communications protocols used between the distinct components of the network.

The Network Security Design specifies the interfaces and services that must be incorporated into the network allowing it to be evaluated as a trusted entity (4:xvi,28). It specifies how the security features are partitioned in the network and how they must interact and be connected for the system to provide C2 service.

It is possible for a LAN to function as a network but not meet the required security architecture. That is, it functions as a LAN but does not utilize the security connections and interactions specified in the Network Security Design Document.

The network system sponsor will provide a test plan including the context in which the testing was or will be conducted. The test plan will identify any and all

interfaces to the NTCB and the network configuration and sizing requirements (4:27).

Summary

This chapter explained NCSC's goals and objectives as they relate to computer security issues and reviewed the four security divisions specified by NCSC (A, B, C and D). This chapter then reviewed in detail the criteria required for a C2 rating. Chapter III will develop the LAN evaluation checklist based on the criteria required for a C2 rating. The checklist can be found in the appendix.

III. Methodology

Overview

A network can be viewed and a security evaluation performed as if it were a system with a single Network Trusted Computing Base (NTCB), or it can be viewed and evaluated as a combination of components, with each component providing a piece or pieces of the NTCB.

In the latter view, once each component is evaluated and assembled into a network, the overall network can be evaluated. The overall evaluation will determine if the individual components work as a logical NTCB and meet NCSC's class C2 criteria. In this way, an overall evaluation for the network can be determined (4:193).

If the former approach is used, a network would have to be evaluated as a total entity. A LAN's configuration can be quite complex with a total LAN evaluation requiring numerous man days. But LAN configurations may change only slightly from installation to installation due to a component required in one installation but not in another. This limited change could be the result of encryption or LAN interconnection requirements.

When a LAN is evaluated by components, a component's evaluation on one installation can carry over to other installations. Only those components not previously evaluated would require a complete component evaluation,

possibly saving time and money. Once all the components of the LAN are evaluated, the system can be evaluated as a composite of distinct components. This final evaluation will determine whether the LAN provides the security features necessary for a C2 rating. To facilitate the component and system evaluations, a checklist has been developed with distinct sections for evaluating the required documentation, each component type and then the total system.

Design Methodology

Evaluating LANs, one component at a time, can provide time and cost savings over evaluating the total system as a whole. The savings are realized by the simplification (breakdown) of a LAN's complex structure and evaluating only those components not previously evaluated. Therefore, when evaluations are performed on similar LANs at different locations, the second and subsequent evaluation would receive significant time and cost savings.

Once the benefits of evaluating a LAN by component were identified, an evaluatable breakdown of the total system had to be developed. There were two possible solutions identified:

1. Separate the LAN into internal and external components. Internal components provide data communications and external components provide subject processing.

2. Separate the LAN based on the types of security relevant mechanisms that must be provided in a C2 system (Discretionary Access Control, Audit and Identification/Authentication).

The first solution was discarded because of the possible overlap in the features provided by the internal and external components. As an example, if a name server was implemented to control access to the LAN it could be a portion of the internal component. The name server would require discretionary access control capabilities to protect its files, audit capabilities to track logons, and identification/authentication mechanisms to authorize use of the LAN. If the name server didn't provide access control for the total system (not a central name server), the above features would also be required on each external component. In this scenario the name server, an internal component, would require the same security capabilities as the external components.

Because of the above problems, the second component breakdown, based on the required security relevant mechanisms, was identified as the most feasible component breakdown structure. The NCSC also identified the second component breakdown as a feasible LAN evaluation mechanism in reference 4.

As specified previously, a C2 system must provide three distinct security mechanisms (Discretionary Access Control, Audit and Identification/Authentication). The LAN can be separated into distinct components by using the required security mechanisms as a guide. This component breakdown leads to three component types:

1. Discretionary Access Control (D) component(s).
2. Audit (A) component(s).
3. Identification/Authentication (I) component(s).

The component can be made up of one or more than one device in each class (D, A and I). The D, A and I components must meet the requirements as specified in chapter II governing the security policy, assurance, accountability and documentation features for a class C2 system. Once the breakdown structure and required security features were identified it was a step by step procedure to design the checklist.

Checklist Design

The checklist is designed to evaluate LANs as a combination of separate and distinct D, A and I components. The checklist identifies security areas that must be evaluated for a C2 rating. The checklist does not specify solutions to meet the criteria, but it is designed to guide the evaluator(s) during the evaluation. The evaluator(s) is responsible for determining if the LAN's capabilities

provide the features necessary to meet each requirement in the checklist.

The checklist is separated into five sections. They are:

I. Required documentation.

II. Discretionary Access Control components (D).

III. Accountability components (A).

IV. Identification/Authentication components (I).

V. Composition of D, A and I components.

After the checklist was defined and validated by AFCSC and HQ USAF/SCTT it was applied to a LAN provided by ESC.

Using the Checklist

Before an evaluation can begin, the sponsor must provide the Security Policy and the Network Security Architecture/Design (NSAD) documents. The documents are used in setting up the LAN and in determining the claimed security capabilities provided by the LAN. It is important to evaluate the documentation's claimed capabilities against the entire checklist. If the documentation's claimed security capabilities do not meet class C2 criteria, there is no reason to continue the evaluation.

The documentation is evaluated in Section I of the checklist. The documentation is further evaluated by comparing the actual capabilities of the components to the capabilities claimed in the documentation. The

documentation to actual component evaluation verifies whether or not the documentation presents an accurate reflection of the component's capabilities.

Section I (Documentation). The Security Policy and the Network Security Architecture and Design (NSAD) documents are evaluated in this section. Section I also requires an evaluation of the Security Policy against Sections II, III, IV and V to determine if the Security Policy's claimed capabilities meet the class C2 criteria. If the claimed capabilities do not meet the C2 criteria, the evaluation should be halted and the sponsor notified.

The Security Policy specifies the secrecy and data integrity policies; for a LAN to receive a C2 rating, both must be provided. The secrecy policy governs the reading of objects; the integrity policy governs writing or modifying objects. The secrecy and integrity policies are provided by Discretionary Access Control (D) components and protection of information while in transit. Discretionary Access Control components require a subject to hold authorization to an object before it can be accessed. Authorizations should be capable of providing access controls at the read (allow read only access) or read/write levels at a minimum.

The Network Security Architecture explains the security-relevant policies, objectives, and protocols (4:28). It provides information on the security features in the network and which devices or pieces of the LAN provide

what security features. It specifies the communications protocols used between the distinct components of the network.

The Network Security Design specifies the interfaces and services that must be incorporated into the network allowing it to be evaluated as a trusted entity (4:xvi). It specifies how the security features are partitioned in the network (component evaluation, D, A, I) and how they must interact and be connected for the system to provide C2 service.

It is possible for a LAN to function as a network but not meet the required security architecture, that is, it functions as a LAN but does not utilize the security connections and interactions specified in the Network Security Design Document. Therefore, the LAN must be installed in adherence to the NSAD.

Sections II, III and IV (Component Evaluation). Sections II, III, and IV of the checklist correspond to the specific features required in the components of a C2 LAN. The LAN must provide discretionary access control (Section II) and the accountability of subjects (Section III). Identification and authentication mechanisms are required for the discretionary access control and accountability features to be effective (Section IV).

Section V (Composition of Components). Section V determines if the component capabilities are carried over

into the consolidated LAN and utilized as stated in the Network Security Architecture and Design documents. It focuses on combining the components in DA, DI, AI, and finally IAD configurations. IAD corresponds to the overall identification-authentication, accountability and discretionary access control criteria required by NCSC. IAD and its required criteria (the security policy, assurance, accountability and documentation features) are the end configuration that a LAN must meet to be eligible for a C2 rating. It is imperative to test for unused interfaces between components and back doors into connected components in this section.

Evaluating a LAN. To evaluate a LAN using the checklist, the documentation section must be completed first and then the security policy should be evaluated against sections II, III, IV and V. If the security policy is deficient when evaluated against the checklist, the deficient areas should be identified and the sponsor notified. If the security policy meets the checklist's requirements, the evaluation can continue.

The hardware and software should be organized into its respective class, D, A or I as specified in the Network Security Design document. The components and the composition of all components should then be evaluated against relevant sections of the checklist and the sponsor's documentation.

No one component is required to meet all areas of the checklist, but the composition of components must satisfy the overall checklist. When Section V is completed, deficient areas in the checklist should be identified, and the sponsor notified. A C2 rating is unlikely without correcting the deficiencies, but there are a few areas that might not apply to all installations. As an example, if the LAN doesn't include encryption, and site security is used in its place, there will be deficiencies concerning encryption that do not affect the security rating.

If all sections of the checklist are completed with Yes answers or a valid alternative is provided for No answers, the LAN can be considered to meet NSA's criteria for a C2 rating. An example of a valid No answer is in Section III.1; audit information is requested for problems with encryption. If encryption is not used on the LAN, a No answer is acceptable. Another example of a valid alternative would be the validation of a component after it is added to the LAN but before it is placed in service (Section II.5, III.4 and IV.4).

Summary

This chapter identified how the checklist was designed and provided instructions on its use. A LAN evaluation accomplished with the checklist only determines a LAN's ability to meet NCSC's criteria for a C2 rating. In this respect, the checklist provides a consistent methodology for

evaluating LANs but doesn't provide approval for a LAN's processing of sensitive or classified information. For a LAN to receive approval for processing sensitive or classified information, an accreditation must also be accomplished. The accreditation determines if all the required security measures are in place and if the overall security risk is acceptable. These measures include physical access control, control of printer output and TEMPEST considerations; AFR 205-16 can provide guidance on accreditation issues. The next chapter discusses the evaluation of ESC's LAN.

IV. Applying the Checklist

Introduction

The checklist provides a simple solution to the complex problem of applying NCSC's criteria to a LAN. The checklist does not specify solutions to meet specific criteria, but it does provide a consistent procedure for LAN evaluations. It easily identifies and isolates the LAN's security deficient areas.

The evaluator(s) is responsible for determining if the LAN's security capabilities meet NCSC's criteria as spelled out in the checklist. Therefore, before an evaluation can begin, the evaluator(s) must understand a LAN's hardware and software capabilities and interactions.

For this evaluation, the documentation providing this information (the Security Policy and Network Security Architecture and Design documentation) was not provided by the sponsor. It is possible for an evaluator(s) to decide the component breakdowns without the Security Policy and NSAD, but it can not be done without extensive knowledge of the LAN's hardware and software capabilities. In an actual evaluation the evaluation process should not continue without the required documents. But to determine the usability of the checklist this evaluation was continued.

In place of the missing documentation, an understanding of the hardware and software capabilities and interactions

was gained by installing and using the LAN. The LAN under evaluation was a scaled down version of ESC's LAN and it consisted of two TEMPEST PCs with LAN interface cards, a central hub and dual fiber optic cable running from each PC to the hub (See Figure 1). One PC is a super station, it shared its application programs and disk space with the second PC.

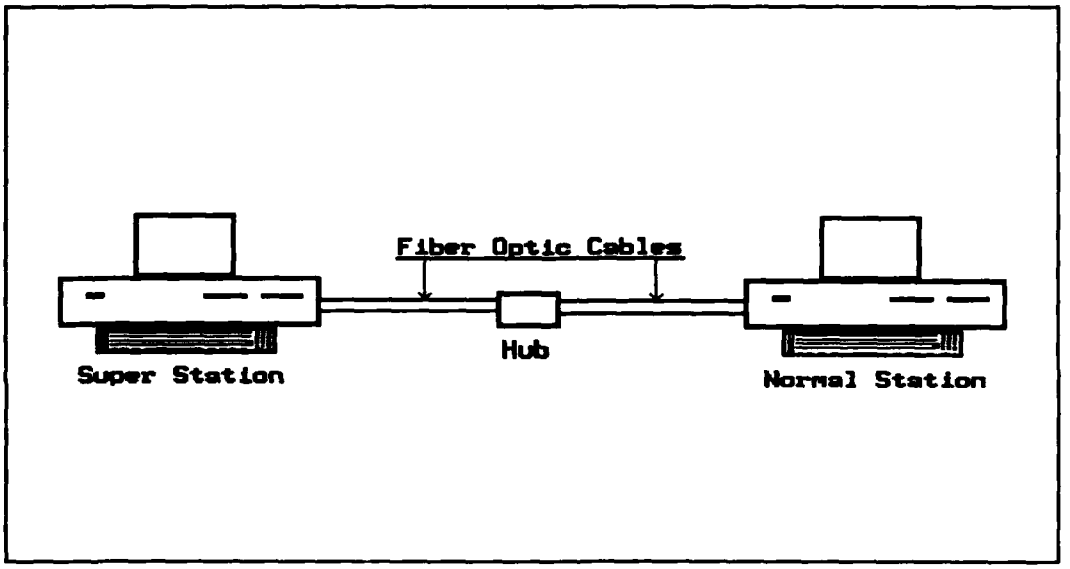

Figure 1. The Evaluated LAN's Architecture

The LAN's normal operating environment utilizes TEMPEST equipment, secure operating locations, and fiber optic cable for LAN communications. Therefore, ESC is not concerned with emanations and their communications media (wireways) are reliable and protected. This LAN's environment was assumed to be identical to the LAN's normal operating environment for evaluation purposes.

Structure of the Evaluation

Once the LAN's hardware and software characteristics were understood, the checklist was applied, starting with Section II. Section I was completed after Sections II, III and IV were completed and a thorough understanding of the total system was obtained. Section V was completed last, as it should be.

Without the required Security Policy and NSAD, the LAN could not reach a C2 rating, but the missing documentation did not impact the final rating. There are numerous other deficient areas; some deficient areas are due to information not provided by ESC/SC-OA and/or the companies providing the hardware and software. Other deficiencies are due to required capabilities which were not provided. The major security deficiencies will be looked at in detail as the checklist is used to complete the evaluation.

Class C2 Discrepancies

Following are the major security deficient areas precluding the LAN from a C2 rating. Questions from the checklist which were marked No are given followed by a description of the problem. A solution to the identified deficiency is identified if possible. Many areas were deficient because a required security capability was not provided. In these cases the corrective measure is obvious, the capability must be provided.

Discrepancies in Section I. This section was accomplished after Sections II, III and IV because the Security Policy and NSAD documents were not provided. By delaying this section, a complete understanding of the features provided by the LAN was applied in place of the documentation.

I.1 Security Policy.

There was no Security Policy identified. By setting up and using the LAN an understanding of the capabilities provided was established.

> Is the data secrecy policy identified?
> (Are users prevented from reading
> unauthorized information?)

This policy was not identified. Users are prevented from reading unauthorized information on the local PCs but there is no secure method for protecting information on remote PCs.

> Is the data integrity policy identified?
> (Is information protected from
> unauthorized modification on processor
> and the network)

The network is in a controlled environment with TEMPEST equipment and fiber optic cable for the transmission path. This environment and inherently reliable media provides good data integrity but there is no protection provided on the processor itself, only on the hard disk.

Is the discretionary access control policy identified? (Individual/Group.)

Only on the local PC, there is no discretionary access control provided on PCs accessed over the LAN (remote PCs).

I.2 Network Security Architecture and Design (NSAD).

This section includes D, A and I components and their interactions. The NSAD was not defined. The features provided were established by installing and using the LAN under evaluation.

The lack of the NSAD and Security Policy was not a factor in this evaluation because the LAN was not close to a C2 rating. If it were, the required documentation would have been invaluable and the evaluation could not have been undertaken without it.

Evaluate the Security Policy against Sections II, III, IV and V. Does it meet the requirements in these Sections?

Since there was no Security Policy this step could not be accomplished. There could be no comparison made between the actual capabilities of the components and their claimed capabilities either.

Discrepancies in Section II. The Discretionary Access Control components discrepancies start here.

II.1 Trusted Facility Manual (TFM) (4:26).

There was not a TFM provided by the sponsor. The closest manual to a TFM was the System Manager's Manual provided by the company furnishing the security software. This System Manager's Manual and the security software applied to a PC's hard disk and did not apply to a LAN environment. To meet the requirements for a TFM, the sponsor should provide a document encompassing the information required in the following section (II.1 in the checklist).

Does the TFM:

> Describe hardware/software that provide D security services including protocols used to export audit data?

The capabilities provided were explained, but there was no explanation of the hardware/software or protocols used and the capabilities were only provided for the local hard disk. The D services must also be provided for remote devices and the local processor's memory and buffers.

> Describe features that should be protected to maintain LAN security?

There was not an explanation of the features requiring protection to maintain LAN security. There were no

features to protect because there was no LAN security. There was a description of the features requiring protection to keep the hard disk secure, but if the hard disk was accessed over the LAN, the security protection mechanism was effectively bypassed.

Explain the security relevant D features and how to utilize them?

Again the features provided at the PC level were explained but there was no security explained or provided at the LAN level.

Describe supported hardware configurations?

The manual covering the LAN covered supported hardware configurations, but not with respect to security. There was no security software provided to control or limit LAN accesses.

Describe security implications of attaching new components?

The security implications of attaching new components was not addressed in the manuals provided.

Describe implications to D components when devices are disconnected or fail?

This area was not addressed in the manuals provided.

Describe component interconnections consistent with overall network architecture?
(Mechanisms and protocols for connecting to A and I components)

There was no overall network security architecture.

Describe loading or modifying network software/firmware?

This was not addressed with respect to security issues. Documentation explained only how to modify or load components.

Describe starting or restarting LAN services to force them into a secure mode of operation?

A description was provided on how to initialize the LAN but there was no security interface provided for the LAN.

Describe physical and administrative environmental controls?
(Supported operating locations)

Physical location and equipment was acceptable, but other daily operating procedures were not provided by ESC/SC-OA for security reasons.

II.2 Is Discretionary Access Control provided?

Discretionary access control is provided but only at the PC level. If the LAN is used to access another PC, the access control procedures on the remote PC are bypassed. The bypassing of the security features on the remote PC is not acceptable. An easily implemented solution would be to require a subject to use the identification-

authentication mechanism on a remote PC before access is granted to any object on that PC.

Can group membership be determined?
(Access can be based on a group identifier but it must be possible to determine group membership)

A group name (identifier) is not used. Users are granted access to everything on the hard disk unless they are specifically denied access. Since there is no group identifier, access is only controlled at the individual level.

Are connections to the A and I components defined?

There are no protocols defined between components.

II.3 Object Reuse (4:20).

Are reused components protected from unauthorized reading?
(Message buffers, Storage devices)

No reused components are protected from unauthorized reading except possibly hard drives, but the hard drive protection can't be relied on because of the unsecured access through the LAN.

Are all previous authorizations revoked prior to a devices (objects) release back to the system?

This capability could be implemented as an external control and the documentation covering operating procedures wasn't provided.

Can a buffer assigned to an internal subject only be reused at the discretion of that subject?

The security capabilities of this system do not allow a subject to set or control reuse of objects. The only object with any protection at all is the hard disk. More protection must be provided for the CPU and hard disk access over the LAN.

II.4 System Architecture (4:23,24).

Does the NTCB maintain a domain for its own execution?

Is the NTCB protected?

The NTCB doesn't maintain a domain for its own execution. It is protected from unauthorized access while it is on the hard disk but not while it is in PC memory.

Are resources protected by the NTCB isolated, protected and subject to DAC and audit requirements?

Not all resources are protected by the NTCB. The hard disk is not subject to the DAC and audit requirements when accessed over the network.

Does the D component meet the stated network security architecture/design?

There is not a NSAD defined.

Are protocols verified or previously tested?
(Normal and abnormal messages in normal and degraded LAN operation)

The protocols are not defined and have not been verified or tested.

II.5 System Integrity (4:24).

> Is hardware/software provided to validate the correct operation of the NTCB? (Protocol to exchange messages between components and verify correct responses)

No, it is not. There is not a NTCB in place on this LAN. The only resource with any protection at all is the hard disk.

> Is the identity and correct operation of a component validated before it is added to the LAN?

Validation of components could be implemented as an external procedure and ESC did not provide their daily operating procedures/instructions.

II.6 Security Testing (4:25).

> Have components interfaces and protocols been tested? (Normal and abnormal conditions in normal and degraded modes)

The interfaces and protocols are not defined.

II.8 Test Documentation (4:27).

There was no documentation explaining testing that was or should be done.

II.9 Design Documentation (4:28).

There was no Design Documentation.

Discrepancies in Section III. This section evaluates the Audit components of the LAN.

III.1 Is audit information provided (4:22,23)?

Yes, but only for applications accessed on a PC via the keyboard. The audit capability is always on for all users. There is no audit trail for access to objects, other than application programs, invoked from the PC security software. Object creation, access and deletion are not included in the audit trail. Actions of system operators/administrators are not tracked other than their use of an application program. If a user or system operator/administrator calls DOS as an application, the audit trail reflects they used DOS but it does not provide any information on the actions taken while using DOS.

Audit information isn't provided for LAN access unless the subject voluntarily uses an application to access the LAN. Voluntary use of the LAN access application cannot be relied on; therefore, actions taken over the LAN cannot be tracked. There are no audit trails kept for problems or errors on the LAN, or modifications or additions to the LAN.

The audit file includes date/time, user identification, application used, and success or failure of logon attempts for those applications that are tracked.

Because of these discrepancies, the audit capabilities of this LAN do not meet the requirements for a C2 rating. The greatest problem is that access to objects (create, access, deletion) and LAN access are not tracked. The lack of audit capabilities in these areas is a major problem and will require a major change to the security software.

III.9 Trusted Facility Manual (4:26).

Again, there was no TFM provided by the sponsor. The manual providing information closest to a TFM was the System Manager's Manual from the company providing the security software. This document provided information on a PC's hard disk security capabilities and not the total LAN. To meet the requirements for a TFM, the sponsor should provide a document furnishing the information required in the Section III.9 of the checklist.

Discrepancies in Section IV. This section evaluates the Identification/Authentication components.

IV.1 Is Identification and Authentication provided?

Yes, but only for access to the local PC. Once access is gained to the local PC, there is no identification-authentication required for access to the LAN or remote PCs.

Is authentication information (group/individual) protected if passed to another device?

No, when another device is accessed, the authentication information is not passed and re-authentication is not required. Not passing authentication information and not requiring re-authentication is a major discrepancy in the security of the LAN. An easy solution to implement would be to require re-authentication when accessing a remote PC.

Is audit data provided via the identified protocol to the A component? (Success/failure of access, date/time user name and location of access)

There is no identified protocol.

IV.9 Trusted Facility Manual (4:26).

The lack of a TFM was covered in Sections II and III and will not be addressed here.

Discrepancies in Section V. Since there were so many No answers in the preceding sections, it is easy to see that this LAN needs many more security capabilities to receive a C2 rating. Some of the deficient areas would require major software changes. An example of an area with major security flaws is provided by the audit component. It needs to be improved drastically in many areas.

Section V provides the evaluation of the overall network composition, but in this evaluation Section V could not be started. There were too many unresolved No answers and there were no components to consolidate or interfaces and protocols to verify. Every question on the checklist in Section V received a No answer.

Summary

The checklist provided a convenient methodology for determining whether a LAN provides security protection at class C2. The checklist does not specify the solution to meet specific criteria, but only the criteria that must be met.

This evaluation started at Section II because of the missing documentation which would have been evaluated in Section I. The LAN did not meet the requirements for a C2 rating in any section of the checklist. The missing documentation added an unforseen complexity in starting the evaluation but it did not affect the final rating.

V. Conclusion and Recommendations

Conclusion

This thesis describes the efforts required to design a checklist used for determining a LAN's capability to provide class C2 security protection. The checklist was reviewed by HQ USAF/SCTT and AFCSC to verify that it provided a complete stand alone procedure for LAN security evaluations at class C2.

There were no changes made to the checklist resulting from the review, but there were some comments about and changes made to the content of the overall document. HQ USAF/SCTT provided constructive comments on the structure of the overall document and provided additional background information on LAN certification and accreditation issues; these issues are addressed in AFR 205-16. AFCSC wanted it understood that the checklist is not an engineering document. It does not provide solutions to meet specific C2 criteria. That is, the checklist identifies the security features (capabilities) that must be provided for a C2 rating, but it does not specify how the security features are to be implemented. Therefore, a thorough understanding of the LAN's security capabilities is a prerequisite in determining if the criteria for a C2 rating are met. The checklist provides a guide for identifying the required capabilities of a C2 LAN, and it is up to the evaluator(s)

to determine if the security capabilities of the LAN meet the criteria for a C2 rating.

The checklist organized the evaluation procedure into a step by step methodology which reduced the possibility of overlooking a risk or discrepancy. Again, the checklist does not provide guidance as to the solution or solutions required to meet specific criteria. The LAN evaluator(s) are responsible for determining if the requirements in the checklist are met by the security capabilities of the LAN.

A LAN evaluation conducted using the checklist provides a procedure unlikely to give a LAN a C2 rating when the LAN does not meet the required criteria. The checklist provides a set evaluation strategy which could standardize the evaluation procedures for LANs at the C2 level. The checklist also gives industry a simple device to measure its hardware, software and documentation. The checklist was arranged with five distinct sections corresponding to:

I. Required documentation.

II. Discretionary Access Control components (D).

III. Accountability components (A).

IV. Identification/Authentication components (I).

V. Composition of D, A and I components.

The checklist was applied against a LAN provided by HQ ESC. ESC's LAN did not include the Security Policy or NSAD documentation required in Section I. In place of the missing documentation, the LAN was installed and used to

develop an understanding of the LAN's capabilities and the component breakdown. With the understanding gained through the hands on environment, the LAN was easily seen to contain many deficient areas precluding a C2 rating and that the missing documentation would make no difference in the overall rating. Therefore, the evaluation was started at Section II and continued in order until Section IV was completed. Section I was then evaluated followed by Section V. A thorough understanding of the LAN was obtained using the modified evaluation order allowing Section I to be completed without the Security Policy and the NSAD.

During the evaluation there were no major problems identified in applying the checklist. A few minor changes were made to checklist's terminology to aid in understanding the criteria's requirements and space for comments was provided by adding an extra line between items in the checklist. If users have trouble understanding the criteria in the checklist, the referrals to reference 4, the Trusted Network Interpretation document, should help.

The overall objective of this thesis effort was the design of the checklist and it was felt an evaluation of the checklist could be accomplished even with a LAN with such limited security capabilities. Normally, the Security Policy and NSAD are required to understand the security features provided, the component breakdown, and interfaces and protocols among the components. But this LAN contained

no overall Security Architecture and Design; it had almost no system security at all. If the LAN had not contained as many deficient areas, the evaluation could not have proceeded without the missing documentation.

The checklist proved to be a simple, straightforward mechanism for evaluating a LAN at class C2. It assists in the security evaluation making it an understandable and straight forward problem. The checklist provides a means of keeping track of what has been done and what needs to be done. The checklist also provides a simple LAN evaluation technique aiding the evaluator(s) in determining what is and is not provided by the NTCB.

The checklist provides a consistent comprehensive methodology for applying NCSC's C2 criteria at all LAN installations. It does not provide specific security features that must be provided to meet class C2, but provides only the criteria that must be met by some implemented security feature. The evaluator(s) must understand the capabilities of the LAN before an evaluation can begin. The final decision on whether the security capabilities of the LAN meet the criteria is left to the evaluator(s). The checklist kept the evaluation procedure organized and on track even with the added complexity of the missing documentation.

Recommendations

This thesis effort developed a functional, standardized procedure (checklist) for evaluating LANs at class C2. The evaluation procedure could be enhanced by placing the checklist in an interactive environment combined with a decision support facility. Justification would be required for each Yes/No answer. The required justification could be used to generate a report on the outcome of the evaluation and the justifications would provide a growing knowledge base showing problems to watch for and possible solutions to the identified problems. The knowledge base would also provide a basis for answering the questions in the checklist (decision support), lessening the subjectivity and increasing the consistency of evaluations.

There should also be standardized procedures developed for LANs and computer systems and at all of NCSC's security divisions. Standardized procedures would provide an evaluator(s) the means to proceed with evaluations in a step by step, consistent manner and limit or eliminate the possibility of missing any security requirements in the evaluation procedure. Standardized procedures would also help industry, by providing a standardized checklist allowing their product development to be evaluated in house as it progresses. Industry and system developers would know at all times where their product stood in relation to the requirements and could consistently apply the criteria in the total life cycle of the product.

Appendix: Proposed Checklist

Section I. Documentation

This section assesses the documentation required for a LAN under evaluation. This section's final requirement is an evaluation of the Security Policy against Sections II, III, IV and V. If the documentation doesn't meet the requirements of the following sections the sponsor should be notified and the discrepancies corrected.

I.1 Security Policy.

	Yes	No
Is the data secrecy policy identified? (Are users prevented from reading unauthorized information)	☐	☐
Is the data integrity policy identified? (Is information protected from unauthorized modification on processor and the network)	☐	☐
Is the discretionary access control policy identified? (Individual/Group)	☐	☐
Are audit capabilities available? (Must include LAN access and all processes started by a user)	☐	☐
Is the information protected on reused components? (Includes message buffers on the LAN)	☐	☐
Evaluate the Security Policy against Sections II, III, IV and V. Does the Security policy meet the requirements in these Sections? (If not notify the sponsor)	☐	☐

I.2 Network Security Architecture and Design (NSAD).

This section includes Discretionary Access Control (D), Audit (A) and Identification/Authentication (I) components and their interactions.

Does the NSAD:

	Yes	No
Describe the security architecture and design?	☐	☐
Describe NTCB partitions/components?	☐	☐
Describe interfaces between NTCB components?	☐	☐
Describe security-relevant policies, objectives, and protocols of components and system?	☐	☐
Describe interfaces and services required to provide security at class C2?	☐	☐
Describe the security functionality of components and the interface between components?	☐	☐
Is it possible to build and evaluate the LAN as specified in the NSAD?	☐	☐

Section II. Discretionary Access Control (D) Components

Information must not be accessible to unauthorized individuals including protection while information is in transit from one location to another. Accessibility includes reading or modifying the object in any way. As an example, if the transmission path is not encrypted the LAN maintenance personnel would require a clearance equal to the information on the LAN. The Discretionary Access Control (D) component must produce audit data for auditable actions performed by the D component and provide the audit data to the Audit (A) component via the identified protocol. Interconnected D components must specify the protocol used to pass user-IDs and file information if this form of communication is allowed. An alternative to passing user-IDs would require the subject to re-authenticate itself for all requests to distinct D components. Re-authentication would require the mechanism and protocol from the Identification/Authentication (I) to Discretionary Access Control components to be invoked at each request for an object from distinct D components.

II.1 Does the Trusted Facility Manual (4:26):

	Yes	No
Describe hardware/software that provide D security services including protocols used to export audit data?	☐	☐
Describe D features that should be protected to maintain LAN security?	☐	☐

	Yes	No
Explain security relevant D features and how to utilize them?		
Describe supported hardware configurations?		
Describe security implications of attaching new D components?		
Describe implications to D components when devices are disconnected or fail?		
Describe D component interconnections consistent with overall network architecture? (Mechanisms and protocols for connecting to A and I components)		
Describe loading or modifying network software/firmware?		
Describe starting or restarting LAN services to force the services into a a secure mode of operation?		
Describe physical and administrative environmental controls? (Supported operating locations)		
II.2 Is Discretionary Access Control provided?		
Can a subject protect created objects? (By default or explicitly)		
Can a subject allow access to created objects in their private data area? (A No answer is allowed)		

	Yes	No
Are only authorized individuals allowed to revoke and grant access to objects?		
Can group membership be determined? (Access can be based on a group identifier but it must be possible to determine group membership)		
Are connections to the A and I components defined?		

II.3 Object Reuse (4:20).

	Yes	No
Are reused components protected from unauthorized reading? (Message buffers, Storage devices)		
Are all previous authorizations revoked prior to a devices (objects) release back to the system?		
Can a buffer assigned to an internal subject only be reused at the discretion of that subject?		

II.4 System Architecture (4:23,24).

	Yes	No
Does the NTCB maintain a domain for its own execution?		
Is the NTCB protected?		
Are resources protected by the NTCB isolated, protected and subject to DAC and audit requirements?		
Does the D component meet the stated network security architecture/design?		

	Yes	No
Does the LAN use NSA approved End-to-End encryption or protected wireways for its communication channels?	☐	☐
Do switches, hubs and media handle only encrypted information or are they in a secure location?	☐	☐
Have protocols been verified or tested? (Normal and abnormal messages in normal and degraded LAN operation)	☐	☐
Do modems or connection devices process only encrypted information or are they in a secure location?	☐	☐
Is the data integrity policy met? (While information is in transit. End-to-End encryption, or acceptable noise levels and reliable media and devices are possible solutions)	☐	☐

II.5 System Integrity (4:24).

Is hardware/software provided to validate the correct operation of the NTCB? (Protocol to exchange messages between components and verify correct responses)	☐	☐
Is the identity and correct operation of a component validated before it is added to the LAN?	☐	☐

II.6 Security Testing (4:25).

Have the D components' interfaces and protocols been tested? (Normal and abnormal conditions in normal and degraded modes)	☐	☐

	Yes	No
Has integrated testing of all D components been accomplished to verify the overall security policy, architecture and design?		

II.7 Does the Security Features Users Guide (4:26):

Describe user visible protection provided by the D components?		
Describe user interface to D components and the interaction among the components?		

II.8 Does the Test Documentation (4:27):

Describe the test plan and test procedures showing how the security mechanisms were or should be tested for the D components and the total system?		
Identify any devices required for testing that are not part of the network and how to use them?		
Describe how all aspects of the Security Policy were tested?		
Describe tests used, including network configuration and sizing?		

II.9 Does the Design Documentation (4:28):

Describe protocol used to pass subject permissions to other D components?		

See section I.2

Section III. Audit (A) Components

Subjects must be accountable for their actions. Subjects are users or other tasks that access and use objects. Accountability is required for all actions that change the state of a protected object or impact the security of the system. The Audit components must have a well defined protocol to accept audit data from the Discretionary Access Control and the Identification-Authentication components.

		Yes	No
III.1	Is audit information provided (4:22,23)?	☐	☐
	Is system administrator able to selectively audit users based on user names?	☐	☐
	Is audit information protected from unauthorized access/destruction?	☐	☐
	Is read access to audit data limited to authorized subjects?	☐	☐
	Is audit information provided for:		
	Identification/Authentication?	☐	☐
	Object read/creation including object name?	☐	☐
	Object modification/deletion including object name?	☐	☐
	Actions of system operators, administrators and security officers?	☐	☐

	Yes	No
LAN access (from, to and user name)?	☐	☐
Date/time stamp of connections?	☐	☐
Exception conditions, transmission errors misrouted packets?	☐	☐
Problems with encryption?	☐	☐
Network configuration changes (devices leaving or being added to the network)?	☐	☐

Does the audit trail provide:

Date/time stamp?	☐	☐
User identification?	☐	☐
Type of event?	☐	☐
Success or failure of the event?	☐	☐
Location (terminal address) of identification/authentication events?	☐	☐

III.2 Object Reuse (4:20).

Are reused A components protected from unauthorized reading? (Message buffers, Storage devices)	☐	☐

	Yes	No
Are all previous authorizations revoked prior to a devices (objects) release back to the system?	☐	☐
Can a buffer assigned to an internal subject only be reused at the discretion of that subject?	☐	☐

III.3 System Architecture (4:23,24).

Does the NTCB maintain a domain for its own execution?	☐	☐
Is the NTCB protected?	☐	☐
Does the A component meet the stated network security architecture/design?	☐	☐

III.4 System Integrity (4:24).

Is hardware/software provided to validate the correct operation of the NTCB? (Protocol to exchange messages between components and verify correct responses)	☐	☐
Is the identity and correct operation of a component validated before it is added to the LAN?	☐	☐

III.5 Security Testing (4:25).

Have the A components' interfaces and protocols been tested? (Normal and abnormal conditions in normal and degraded modes)	☐	☐

	Yes	No
Has integrated testing of all A components been accomplished to verify the overall security policy, architecture and design?		

III.6 Does the Security Features Users Guide (4:26):

Describe user visible protection provided by the A components?		
Describe user interface to the A components and the interaction among them? (Including audit capabilities)		

III.7 Does the Test Documentation (4:27):

Describe the test plan and test procedures showing how security mechanisms were or should be tested for the A components and the total system?		
Identify any devices required for testing that are not part of the network and how to use them?		
Describe how all A capabilities of the Security Policy were tested?		
Describe tests used, including network configuration and sizing?		

III.8 Design Documentation (4:28,221).

Is the protocol used to import audit data from D and I components described and well defined?		

See section I.2

III.9 Does the Trusted Facility Manual (4:26):

	Yes	No
Describe hardware/software that provides audit services including detailed structure for each type of audit record?		
Describe the A features that should be protected to maintain LAN security?		
Explain security relevant A features and how to utilize them?		
Describe supported hardware configurations?		
Describe security implications of attaching A components?		
Describe implications to A components when devices are disconnected or fail?		
Describe A component interconnections consistent with overall network architecture? (Mechanisms and protocols for receiving data at A components)		
Describe loading or modifying network software/firmware?		
Describe starting or restarting LAN services to force them into a secure mode of operation?		
Describe physical and administrative environmental controls? (Supported operating locations)		

Section IV. Identification/Authentication (I) Components

Identification/Authentication components must provide the identification and authentication mechanism for the system. It provides all the Identification/Authentication services and must have a well defined protocol for passing this information to the Discretionary Access Control (D) and Audit (A) components to complete the overall Security Policy. The Identification/Authentication component can be invoked every time a new D component is accessed or, mechanisms and protocols can be in place to pass user-IDs through the LAN in some type of reliable mode.

		Yes	No
IV.1	Is Identification and Authentication provided?	☐	☐
	Are there individual user names?	☐	☐
	Is there a unique user authentication mechanism required?	☐	☐
	Is authentication data protected from unauthorized access?	☐	☐
	Is authentication information (group/individual) protected if passed to another device?	☐	☐
	Is audit data provided via the identified protocol to the A component? (Success/failure of access, date/time user name and location of access)	☐	☐

IV.2 Object Reuse (4:20).

	Yes	No
Are reused components protected from unauthorized reading? (Message buffers, storage devices)	☐	☐
Are all previous authorizations revoked prior to a device's (objects) release back to the system?	☐	☐
Can a buffer assigned to an internal subject only be reused at the discretion of that subject?	☐	☐

IV.3 System Architecture (4:23,24).

Does the NTCB maintain a domain for its own execution?	☐	☐
Is the NTCB protected?	☐	☐
Are resources protected by the NTCB isolated, protected and subject to DAC and audit requirements?	☐	☐
Does the I component meet the stated network security architecture/design?	☐	☐

IV.4 System Integrity (4:24).

Is hardware/software provided to validate the correct operation of the NTCB? (Protocol to exchange messages between components and verify correct responses)	☐	☐
Is the identity and correct operation of an I component validated before it is added to the LAN?	☐	☐

IV.5 Security Testing (4:25).

	Yes	No
Have the I Components interfaces and protocols been tested? (Normal and abnormal conditions in normal and degraded modes)	☐	☐
Has integrated testing of all I components been accomplished to verify the overall security policy, architecture and design?	☐	☐

IV.6 Does the Security Features Users Guide (4:26):

Describe user visible protection provided by the I components?	☐	☐
Describe user interface to I components and the interaction among the components?	☐	☐

IV.7 Does the Test Documentation (4:27):

Describe the test plan and test procedures showing how security mechanisms were or should be tested for the I components and the total system?	☐	☐
Identify any devices required for testing that are not part of the network and how to use them?	☐	☐
Describe how all aspects of the Security Policy were tested?	☐	☐
Describe tests used, including network configuration and sizing?	☐	☐

IV.8 Design Documentation (4:28,221).

	Yes	No
Is the protocol used to export authenticated IDs to other components well defined.		

See section I.2

IV.9 Does the Trusted Facility Manual (4:26):

Describe hardware/software that provide I security services including protocols used to export audit data?		
Describe I features that should be protected to maintain LAN security?		
Explain security relevant I features and how to utilize them?		
Describe supported hardware configurations?		
Describe security implications of attaching I components?		
Describe implications to I components when devices are disconnected or fail?		
Describe I component interconnections consistent with overall network architecture? (Mechanisms and protocols for sending data to A components and authenticated IDs to D components)		
Describe loading or modifying network software/firmware?		

	Yes	No
Describe starting or restarting LAN services to force them into a secure mode of operation?		
Describe physical and administrative environmental controls? (Supported operating locations)		

Section V. Overall Network Composition

First, determine if there is a YES answer for each question in Sections I, II, III and IV. If not, identify the deficient areas and determine if they must be corrected. If corrections are required notify the sponsor.

Once deficient areas are corrected or explained, Section V can be completed. Combine distinct components into their respective group, D, A or I. The collection of components in each group (D, A or I) must continue to meet its respective criteria as specified in the checklist.

Connected Discretionary Access Control (DAC) components must support the same identification passing protocol. When connected, a component composed of two or more components must support the identification passing protocol of the target network architecture. The DAC policy provided by this new component must also support the target network DAC policy (4:197).

Audit components support a set protocol for receiving audit information from other components. The collection of Audit (A) components must maintain the protocol and support the audit policy of the network (4:198).

Identification/Authentication components support protocols to facilitate information passing to DAC and Audit components. The collection of Identification/Authentication components must maintain the network protocol for communicating with DAC and Audit components (4:198).

There can be overlap in the security features provided but there can not be any loop holes or back doors added when the equipment is consolidated into a LAN. This is a critical issue and should receive additional emphasis!

		Yes	No
V.1	Were the component capabilities evaluated against the documentation's claimed capabilities?	☐	☐
V.2	Is there a Yes answer for every question in Sections I, II, III and IV, if not are the deficient areas satisfied in another way?	☐	☐
V.3	Does the composition of D components maintain the requirements of Sections I and II?	☐	☐
V.4	Does the composition of A components maintain the requirements of Sections I and III?	☐	☐
V.5	Does the composition of I components maintain the requirements of Sections I and IV?	☐	☐
V.6	Composition of D and I components, DI (4:200).		
	Is the network DAC policy maintained?	☐	☐
	Are the interfaces/protocols to the A component maintained?	☐	☐
	Are identification/authentication (I/A) services provided to other components using well defined, protected protocols?	☐	☐

V.7 Composition of D and A components, DA (4:201).

	Yes	No
Is the network DAC policy maintained?	☐	☐
Are the interfaces/protocols to the I component maintained?	☐	☐
If A services are provided to other components, does the interface/protocol support the network audit policy?	☐	☐

V.8 Composition of I and A components, IA (4:202).

Are the I and A interfaces and protocols in place and correct? (Must be able to import audit and identification/authentication data and export authenticated user-IDs)	☐	☐

V.9 Composition of I, A and D components, IAD (4:204).

Does the IAD composition meet the composition rules for DI, DA and IA compositions?	☐	☐
If the IAD component supports directly connected users, does it meet the C2 criteria? (To support directly connected users it must be able to stand on its own)	☐	☐

Bibliography

1. Department of Defense. Proceedings of the Department of Defense Computer Security Center Invitational Workshop on Network Security. New Orleans, La. DoD Computer Security Center. Fort Meade Md, March 1985.

2. Department of Defense. Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements. CSC-STD-004-85 DoD Computer Security Center. Fort Meade Md, June 1985.

3. Department of Defense. Trusted Computer System Evaluation Criteria. DOD 5200.28-STD. Washington DC: DoD, December 1985.

4. National Computer Security Center. Trusted Network Interpretation of The Trusted Computer System Evaluation Criteria. NCSC-TG-005. National Computer Security Center. Fort Meade Md, 31 July 1987.

VITA

Captain Rick E. Whitson [redacted] In December 1977 he enlisted in the Air Force and in February 1978 he was an Honor Graduate from basic training. In 1981 he was accepted into the Airman's Education and Commissioning Program (AECP) and enrolled in the University of Puget Sound, Tacoma, Washington. He received a Bachelor of Science in Computer Science/Mathematics in 1983 and was designated a Distinguished Graduate by the Air Force Institute of Technology, Civilian Institution Programs. He received his commission after attending Officer Training School and graduated as a Distinguished Graduate in September 1983. His first assignment as a commissioned officer was to the 7th Communications Group, Pentagon, Washington D.C. He served there until attending Squadron Officer School in March 1987. He graduated from Squadron Officer School in May 1987 as a Distinguished Graduate and immediately entered the School of Engineering, Air Force Institute of Technology.

[redacted]

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

ADA202536

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) AFIT/GCS/ENG/88D-23	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION School of Engineering 6b. OFFICE SYMBOL (If applicable) AFIT/ENG	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) Air Force Institute of Technology Wright-Patterson AFB, Oh. 45433-6583	7b. ADDRESS (City, State, and ZIP Code) 10 Jan 89
8a. NAME OF FUNDING/SPONSORING ORGANIZATION HQ ESC 8b. OFFICE SYMBOL (If applicable) SC-OA	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code) San Antonio, Tx 78243-5000	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)
A CLASS C2 SECURITY EVALUATION PROCEDURE FOR LOCAL AREA NETWORKS — UNCLASSIFIED

12. PERSONAL AUTHOR(S)
Rick E. Whitson, Capt, USAF

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
MS Thesis	FROM _____ TO _____	1988 December	79

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Computer Networks Security
12	07		

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

Thesis Chairman: Bruce L. George, Capt, USAF
Assistant Professor of Electrical Engineering and Computer Science

Abstract:

The National Computer Security Center's Computer Security Requirements, CSC-STD-003-85 (Yellow Book) specifies "Class C2" as the required protection level for computer systems running at a "system high" level of Top Secret. Methodology exists to determine if a computer system provides class C2 protection, however, there are no general procedures available to determine if a Local Area Network (LAN) provides class C2 protection.

This thesis effort reviewed the criteria necessary for a C2 rating and developed a checklist based on the three types of security features

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS	UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Capt Bruce L. George	22b. TELEPHONE (Include Area Code) (513) 255-3576 / 22c. OFFICE SYMBOL AFIT/ENG

DD Form 1473, JUN 86 — Previous editions are obsolete. — SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

Block 19 cont,

required (discretionary access control, identification/authentication and audit capabilities) in a C2 system. HQ USAF/SCTT and the Air Force Cryptologic Support Center (AFCSC) reviewed the proposed checklist to identify deficiencies and inconsistencies. Their comments were addressed and the checklist modified as required. The checklist was then applied to a LAN used in the US Air Force to verify the capabilities of the checklist and determine if the LAN provided class C2 protection. Problems in applying the checklist were identified and the changes were incorporated into the checklist. The checklist can now be used to determine if a LAN provides class C2 security.